We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

5,500
Open access books available

136,000
International authors and editors

170M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter

An Emphasis on Quantum Cryptography and Quantum Key Distribution

Bharadwaja V. Srividya and Smitha Sasi

Abstract

The application of internet has spiked up in the present-day scenario, as the exchange of information made between two parties happens in public environment. Hence privacy of information plays an important role in our day to day life. There have been incredible developments made in the field of cryptography resulting in modern cryptography at its zenith. Quantum computers are one among them creating fear into security agencies across the world. Solving the complex mathematical calculations is uncomplicated using quantum computers which results in breaking the keys of modern cryptography, which cannot be broken using classical computers. The concept of quantum physics, into the cryptographic world has resulted in the advancement of quantum cryptography. This technique utilizes the idea of key generation by photons, and communicates between peer entities by secured channel. Quantum cryptography adapts quantum mechanical principles like Heisenberg Uncertainty principle and photon polarization principle to provide secure communication between two parties. This article focuses on generation of a secret shared key, later converted into Quantum bits (Qbits) and transmitted to the receiver securely.

Keywords: quantum cryptography, Q bits, dirac vector notation, key distribution, secure transmission

1. Introduction

Cryptography is dexterity of solving and writing codes. Cryptography is used in secured communication between peer parties. A cryptosystem is a network security model, which consists of design and implementation of cryptographic algorithms and associated frame work to contribute towards providing security for information. Basic Model of cryptosystem shown in **Figure 1** [1].

Network Security elements:

The important elements of cryptosystem are described –

- **Plain text:** This is the original data that needs to be secured over the unreliable channel.

- **Encryption Algorithm:** It is a mathematical model, which converts original plain text to cipher text, by using encryption key.

IntechOpen

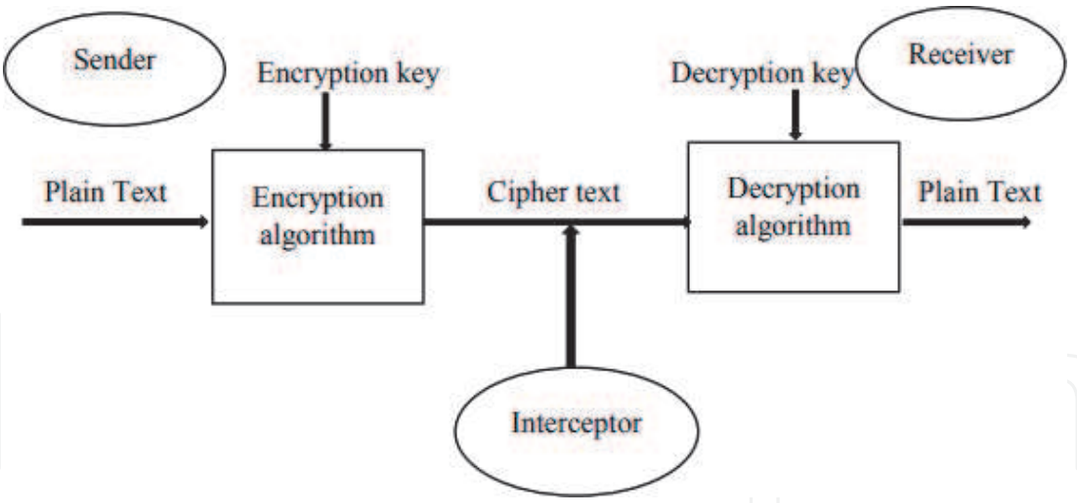

Figure 1.
Basic model of the cryptosystem.

- **Cipher text:** The output generated by the mathematically oriented encryption algorithm is commonly referred to as cipher text. The cipher text is communicated to the peer over an unreliable channel.

- **Decryption Algorithm:** It is a inverse mathematically oriented algorithm which converts the cipher text to plaintext by using the appropriate decryption key.

- **Encryption Key:** It is an arbitrary value generated by the transmitter. This value helps in converting the original data to the scrambled version of the plain text by using an encryption algorithm.

- **Decryption Key.** It is a value shared to the receiver in case of shared key cryptosystem or mathematically generated by receiver in case of public key cryptosystem. This decryption key helps to convert the scrambled version of the plaintext to the original data.

- **Key Space:** This is a sample space consisting of all possible types of keys.

- An **interceptor** (an attacker) is an illegitimate peer who endeavors to detect the original data. This unauthorized peer may be aware of the decryption algorithm. But without the knowledge about the appropriate key, the decryption fails.

Types of Cryptosystems

Cryptosystems are undoubtedly classified as two types namely: Symmetric Key Encryption and Asymmetric Key Encryption.

Symmetric Key Encryption

The process of enciphering and deciphering, utilizes the same shared key for in this cryptosystem. It is also known as secret key cryptosystem. The popular cryptosystem methods are:

- Digital Encryption Standard (DES),

- Triple-DES (3DES),

- Advanced Encryption Standard (AES)

- IDEA
- BLOWFISH.

Asymmetric Key Encryption

The process of enciphering and deciphering utilizes different, but mathematically related pair of keys, in this cryptosystem. The popular algorithms are:

- Elliptic Curve Cryptography (ECC)
- RSA

However, as the data and innovation is expanding, traditional cryptographic methods are inadequate in giving the protection. Later quantum computation and quantum cryptography with quantum mechanics can be utilized to do the appropriation such that security cannot be traded off among clients. The methodology is known as quantum cryptography or quantum key distribution [2].

2. Recent trends in cryptography

2.1 Dirac vector notation

Dirac vector notation or Bra-ket notation is a standard way of representing classical bits as a vector [3, 4]. A Cbit (Special case of Qbit vectors) with a value 0 can also be written as $|0\rangle$ or $\begin{pmatrix}1\\0\end{pmatrix}$..

A Cbit with a value 1 can also be written as, $|1\rangle$ or $\begin{pmatrix}0\\1\end{pmatrix}$.

Tensor product of vectors is given as,

$$\begin{pmatrix}x_0\\x_1\end{pmatrix}\otimes\begin{pmatrix}y_0\\y_1\end{pmatrix}\text{-}\begin{pmatrix}x_0\begin{pmatrix}y_0\\y_1\end{pmatrix}\\x_1\begin{pmatrix}y_0\\y_1\end{pmatrix}\end{pmatrix}\text{-}\begin{pmatrix}x_0y_0\\x_0y_1\\x_1y_0\\x_1y_1\end{pmatrix}\text{ and }\begin{pmatrix}x_0\\x_1\end{pmatrix}\otimes\begin{pmatrix}y_0\\y_1\end{pmatrix}\otimes\begin{pmatrix}z_1\\z_2\end{pmatrix}$$

$$=\begin{pmatrix}x_0y_0z_0\\x_0y_0z_1\\x_0y_1z_0\\x_0y_1z_1\\x_1y_0z_0\\x_1y_0z_1\\x_1y_1z_0\\x_1y_1z_1\end{pmatrix}$$

2.2 Qbits

The Cbit vectors shown above are special cases of Qbit vectors. A Qbit comprises of 0 or 1. This is called superposition. In simpler words superposition means the Qbit is both 0 and 1 at the same time. A Qbit is represented by $\begin{pmatrix} a \\ b \end{pmatrix}$ where a and b are complex numbers and, $\|a\|^2 + \|b\|^2 = 1$.

Examples of some Qbits are [5, 6],

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} -1 \\ 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$$

During the measurement of the Qbit, it yields the actual value 0 or 1. This result is generally obtained at the termination of the Quantum computation. As mentioned a Qbit has a value $\begin{pmatrix} a \\ b \end{pmatrix}$ which then encodes to 0 with a probability $\|a\|^2$ and 1 with a probability $\|b\|^2$. The Qbit $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ has a 100% chance of collapsing to 0 and Qbit $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ has a 100% chance of collapsing to 1 [5].

2.2.1 Operations on Qbits

To measure and operate on Qbits different gates are used in the form of matrices. These Matrix operators are used to design device, and manipulates Qbit spin/polarization without measuring and collapsing it. There are numerous popular matrix operators that can be used in Quantum computation. Quantum computing use only reversible operations [7]. Reversible means given the operation and output value, you can find the input value, For Ax = b, given b and A, you can find x [2].

2.2.1.1 Hadamard (H) gate

Hadamard gate works on a single Qbit. It helps in creating superposition; where during measurement the probability of getting 0 or 1 is equal. The Hadamard gate takes a 1 or a 0 bit and disseminate it into exactly equal superposition. It comprises of two rotations π about the z-axis and $\frac{\pi}{2}$ about the y- axis. The H gate shown in **Figure 2** [2]. Hadamard matrix is given by

$$\mathrm{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Figure 2.
H-gate.

2.2.1.2 Controlled not-gate

Controlled "Not-gate" operates on bit-pairs, commonly referred to as "Control bit" and "Target bit". The condition over bit-pairs are:

- Control-bit = 0; Then Target bit is "unchanged"
- Control-bit = 1: Then the Target bit is "Flipped"

In the binary pair shown, the most significant bit is referred to as control bit and the least significant bit as the target bit. The CNOT gate shown in **Figure 3** [2].

$$\begin{aligned} 00 &\rightarrow 00 \\ 01 &\rightarrow 01 \\ 10 &\rightarrow 11 \\ 11 &\rightarrow 10. \end{aligned}$$

It is represented by the matrix,

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

2.3 Quantum entanglement

Quantum Key Distribution is also based on Quantum Entanglement principle according to which two particles can be entangled such that when of property is measured, on either of the particle the opposite state will be obtained on the entangled particle. This is totally independent of distance between particles, also the key feature of this is that, it is impossible to measure the state prior until it is discussed over classical channel [8].

2.4 Bloch sphere

It is used to represent states of qbit on a unit sphere. The operations performed on qbit during qbit information processing is described in block sphere. The Bloch Sphere Representation is shown in **Figure 4** [1].

Representation of single qbit state is given by:

$$|\varphi> = e^{i\gamma}\left(\cos\frac{\theta}{2}|0> + e^{i\emptyset}\sin\frac{\theta}{2}|1>\right)$$

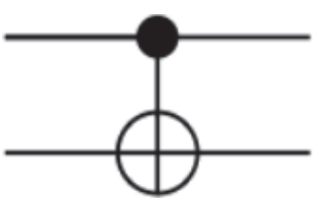

Figure 3.
CNOT-gate.

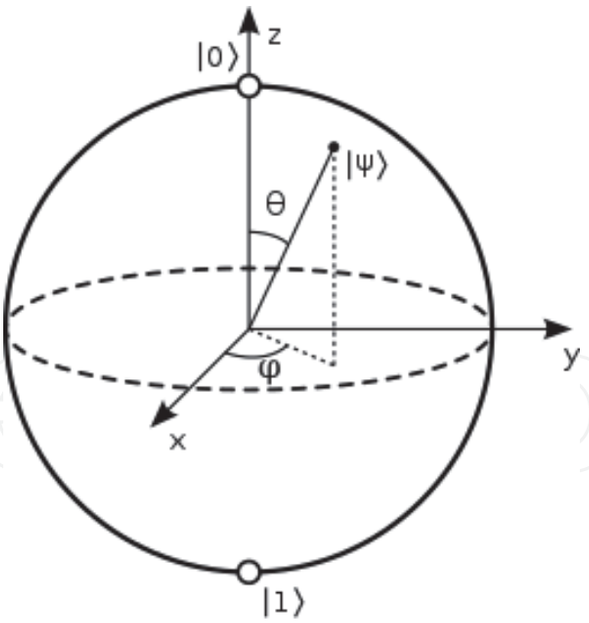

Figure 4.
Bloch sphere representation.

Where γ, θ, φ are real numbers.

Bloch sphere is general representation of complex number z where $|z^2| = 1$ as point on circle in complex plane.

General Qbit: $|\Psi > = \alpha |0 > + \beta |1>$.

2.5 BB84 protocol

BB84 was invented by Charles Bennet and Gills Brassard in 1984. This is first security protocol that was designed to implement QKD which uses idea of photon polarization. The key is transmitted as number of binary bits which are encoded on a random polarization basis [9].

In this protocol there are two channels used mainly for transmission.

1. Quantum Channel
2. Classical Channel

Quantum channel is the one that is used to transmit secure information by converting into bits and transform information photons which is quantum information. This channel can be used to transmit classical information as well. Classical channel is the one that is used to transmit classical information. Examples include e-mail, message, phone lines etc. This protocol is mainly based on Heisenberg uncertainty principle that states measuring quantum state without disturbing is impossible. Hence introducing anomaly by intruder can be noticed by the user [2]. The quantum Key distribution is as shown in **Figure 5**.

2.5.1 Working

The **Figure 5** illustrates that Quantum Key Distribution system has two channels i.e. quantum channel and public channel. Quantum Channel is used to transmit and share the information of.

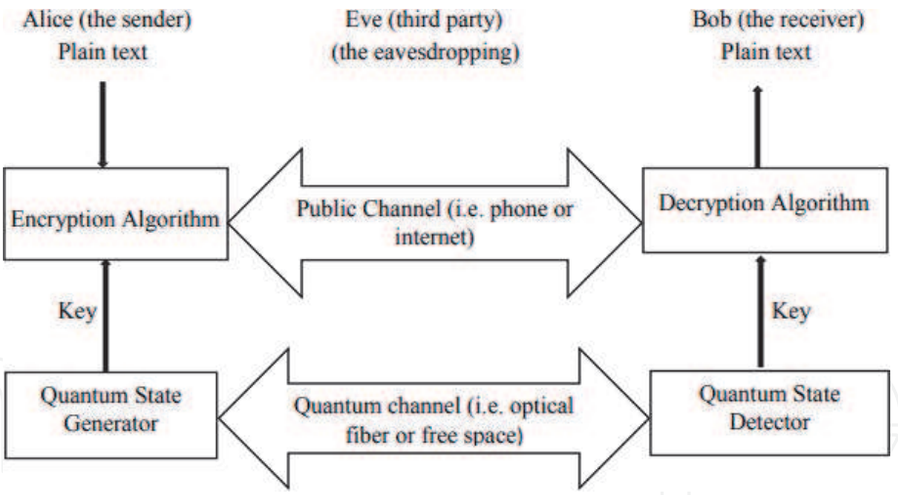

Figure 5.
Quantum key distribution.

Secret key in the form of polarized photon, called as quantum bit (qbit). In the meantime the open channel is utilized to examine the procedure of qbits transmission and make an arrangement about the mutual mystery key. For the most part, there are two medium kinds of quantum channel which is executed on QKD framework for example optical fiber and free space [10].

There are some famous character terms that is utilized in QKD framework to be specific Alice as the sender, Bob as recipient, and Eve as meddler. Quantum condition of photon is utilized to recognize nearness of outsider. The message is transmitted by means of polarization photon meant by zero or one that has one piece quantum data called as qbit. The sender transmits energized photon through quantum channel utilizing channel on arbitrary premise. Likewise beneficiary uses irregular channels to get the information and after that check for change in got bits.

There are two steps involved in key distribution

1. One-way Communication (Via quantum Channel)

   Step 1: user A (Alice) randomly chosen polarized photon and send it to user B (Bob) over Quantum channel.

   Step 2: In this, user B receives photons using random basis either rectangular or diagonal.

2. Two-way Communication (Via Public channel)

   Step 1: User A will use public channel to inform user B about the polarization she chose for every bit sent to user B without disclosing the bit value.

   Step 2: Now user B will compare the polarization sequence he received from user A with the sequence he generated.

   Step 3: Bits of same orientation of those two sequences can be used as secret key.

2.5.1.1 Post reception

a. Error Estimation:

   Both sender and receiver discusses the basis used through a classical channel which is either through a e-mail, telephone. Then discards the bits which basis are not matched.

Whenever there is an intrusion, error is introduced and keys with users does not match. Hence errors are to be considered, if it exceeds QBER Threshold then key is discarded and recent.

b. Error correction:

This is performed by considering bits at both sender and the receiver by removing errors in key using certain protocols namely cascade, winnow. QKD is a technique that creates symmetric key by using quantum properties of light to communicate between users.

2.5.2 Eaves dropping

If attacker (eve) tries hacking the bits secretly that is if he/she tries to tap channel then that is observed at the receiver end. According to No Cloning theorem, an unknown quantum state cannot be cloned therefore eve cannot have same information as Bob Probability of Eavesdropping [11]:

$$\text{For N bits} = (3/4)^{N}$$

When N increases, detecting eavesdropping is also easier.
Advantages:
Detection of Eavesdropping
Disadvantages:
Loss of photon in transmission.

2.5.3 Photons

The basic unit of the electromagnetic radiation is the photons. The classical computer uses bits to transfer the data, while quantum computing is based on quantum mechanics which make use of photons for communication. Qbits can be combination of both 0 s and 1 s having more than one state, such that retrieving the information about one qbit will give the result of other states too, unlike the classical computing where 0's and 1's are used [12].

2.5.4 Essentials of QKD

The fundamental principles of Quantum Key Distribution protocol is based on the two Quantum mechanics laws.

According to Heisenberg Uncertainty without operating the system, it is not possible to carry out any sort of measurement on the system. For example, consider the two conjugate variables having momentum p and position x, both parameters cannot be measured concurrently [12].

Zurek and Wooters presented the first polarization principle on photons in the year 1972. According to this principle and also no-cloning theorem, any eaves dropper will not be able to duplicate the random qbits. This principle elaborates about polarization of light photons and its orientation in a specific direction. Photon destruction can result due to the utilization of erroneous photon filters. In cloning theorem, if the state of photon orientation are distorted, then passive attack of the system may occur. Therefore Quantum Mechanics key distribution recommends security.

2.5.5 Heisenberg uncertainty principle

The impact of Heisenberg Uncertainty Principle is huge just for movement of infinitesimal articles and is insignificant for that of plainly visible items. The Heisenberg Uncertainty Principle expresses that it is difficult to know at the same time the precise position and force of a particle. That is, the more precisely the position is resolved, the less known the force, and the other way around. This standard is not an announcement about the points of confinement of innovation, yet a crucial farthest point on what can be thought about a particle at some random minute. This vulnerability emerges in light of the fact that the demonstration of estimating influences the item being estimated. The best way to gauge the situation of something is utilizing light, at the same time, on the sub-nuclear scale, the collaboration of the light with the article unavoidably changes the item's position and its course of movement [13].

Under the laws of quantum physics, a moving photon has one of four introductions; vertical, horizontal, or diagonal in opposing directions as shown in **Figure 6**. Quantum cryptographic gadgets transmit photons each one in turn, and every photon has a specific introduction. Photon sniffers can record the introduction of every photon, except in certain situations. Because as per Heisenberg's uncertainty guidelines, doing so will change the introduction of a portion of the particles which will caution both the sender and the receiver that their channel is being examined. Heisenberg's vulnerability rule is of gigantic advantage to information security that, if quantum cryptography is utilized to send keys by means of photons at that point consummate encryption is guaranteed.

2.5.6 Photon polarization

Basically polarization of light wave is restricting plane of vibration of electric field in a definite plane. There are 3 types of light polarization:

1. Plane polarized light

2. Circularly polarized light

3. Elliptical polarized light

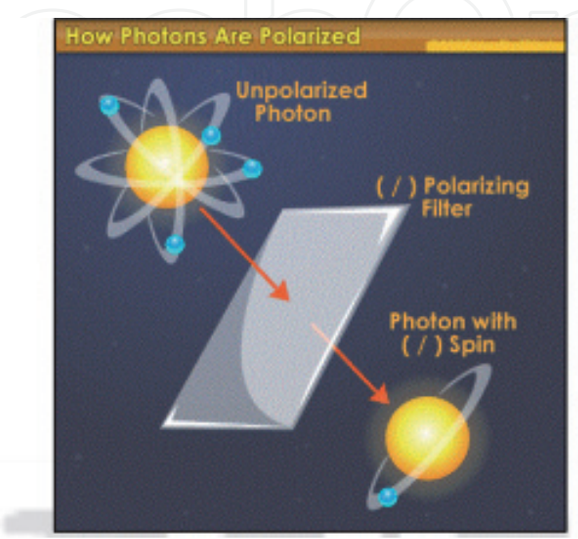

Figure 6.
Polarization of photons.

A device called a Polarizer allows us to place a photon in a particular polarization. A Pockels.

Cell can be used too. The polarization basis is mapping we decide to use for a particular state.

There are two types of Basis/Polarizer through which polarization can happen (**Table 1**),

1. Rectilinear Basis

2. Diagonal Basis

Spin of Rectilinear Basis,
If $\theta = 0°$ $\rightarrow State|0\rangle$
$\theta' = 90°$ $\rightarrow State|1\rangle$

Spin of Diagonal Basis,
If $\theta = 45°$ $\rightarrow State|0\rangle$
$\theta' = 135°$ $\rightarrow State|1\rangle$

		0	1
Rectilinear Basis			
Diagonal Basis			

Table 1.
Polarization using basis.

Photon polarization principle explains how photons can be oriented in different directions. Polarized photons can be detected only with photon filter of correct polarization otherwise photon will be destroyed. Plane polarization of light can be done by ways like reflection, refraction, selective absorption, scattering, double reflection. In circularly and elliptically polarized light, electric field of light is confined in one direction but direction rotates as light propagates.

2.5.7 No cloning theorem

The eminent feature distinguishing between classical and quantum theory is No cloning theorem which restricts copying of quantum state.

Cloning in physics means much perfector copy where the reality of positions and momenta and energy levels of every particle and interaction are exactly the same in the copy as the original.

No cloning preliminaries:

Quantum properties that needs to be known:

1. Super positions

   Particles can be in several states at once, in quantum mechanics the whole is the sum that is the superposition of its different possible parts

   $|A> = |A> + |A>$

2. Composite systems

   The superposition of the product of component.

   $|AB> = |A> + |B>$

3. Transformations distribute

   Any change to a particle that in superposition of a state affects all of the states independently.

   $T(|A1> + |A2>) = T(|A>) + T(|A>)$

No cloning theorem states that "an identical copy of unknown quantum state cannot be created".

2.5.8 Quantum channels

The communication for quantum network over optical networks and photon based qbits for wide range distances are used. Optical networks support the wide range of bandwidth. The Quantum bits can be transmitted reliably and at high velocity over an optical fiber channel.

2.5.9 Fiber optic networks

To design and implement Optical networks the contemporary Telecommunication equipment's can be utilized. At the transmitter, a unique photon source can be produced by densely attenuating a standard telecommunication laser such that the average number of photons per pulse is below 1. The receiver can have an avalanche photo detector. For the phase and polarization control, beam splitters and interferometers are used. Entangled photons are generated through continuous parametric down conversion of entanglement based protocols.

2.5.10 Free space networks

Fiber optic networks works based on free space quantum networks, but rely online of sight between the communicating parties. Free space networks provides higher bandwidth and better data rate than fiber optic networks and this does not have polarization scrambling like optical fiber.

2.5.11 Cavity-QED networks

Quantum key distribution based on Telecommunication lasers and parametric down converters is combined with photo detectors. To amalgamate and retransmit the quantum data, without disturbing the current states, is important in distributed quantum entangled system. Cavity quantum electrodynamics (Cavity QED) helps to generate such quantum entangled system. In this method, the quantum states can be transmitted to and from one atomic quantum states which is located in single atom and consists of optical cavities. This process supports transmission of quantum states between atoms over optical fiber for the creation of remote entanglement distributed systems [14].

3. Pros and cons of QKD

Quantum key distribution is a one of the techniques used for exchanging keys between two users. The main advantage of quantum communication is its security. Since any change made to a particle of an entangled pair is reciprocated by the other, quantum information secured through quantum cryptography cannot be tapped. This is also because of the no cloning and no destroying theorem. So the information can neither be duplicated nor be destroyed. Discrete variable QKD is limited to around 200 km until a quantum repeater is created and can be efficiently implemented. This currently requires a quantum memory. Continuous variable QKD is also limited to similar distances and cannot pass an Optic amplifier in a standard communication network yet also has no known repeater architecture. This will have to be overcome for global QKD to be taken up. There is a trade-off in speed over distance. The longer the distance, the slower the quantum communication. Therefore classical communication is currently faster and can propagate over global distances. It is possible satellite based QKD will allow longer distance quantum communication but this has not been performed to date. When sending quantum information one must also have some classical communication to ensure security, which means that both a classical and quantum network must exist side-by-side.

Despite these advantages, the technology needed to build a quantum computer is currently beyond our reach. This is due to the fact that the coherent state, fundamental to a quantum computers operation, is destroyed as soon as it is measurably affected by its environment. Attempts at combating this problem have had little success, but the hunt for a practical solution continues.

QKD is advantageous when compared with conventional cryptographic techniques in certain aspects which are as follows:

1. Any attempts of eve in obtaining information can be identified with the help of two principles of quantum mechanics.

2. Quantum key distribution protocol can detect eavesdropping because the error level is more during this case.

3. The errors caused during communication between users can be detected.

4. Video can be transferred between the nodes with the rate of 128–1024 kbps without the consideration of any overhead data.

5. QKD generates new private key randomly and continuously so it is next to impossible to steal any key distributed by quantum cryptography.

6. Data security is increased with QKD protocol.

7. The actual information can never be revealed to any third party.

8. Security of QKD is based on the laws of quantum physics which can be proven.

QKD sounds too good when concerned with security but when it comes to practical considerations it takes back seat. There are certain technical weaknesses related to implementation.

1. High set up and installation cost for commercial use.

2. Long distance transmission is not feasible, range of QKD is restricted to few hundred kilometers and quantum repeaters do not have any practical application.

3. Equipment set up has to be done precisely.

4. Key distribution rate of QKD is 1000 to 10000 times slower than the conventional optical communication.

5. While transmitting video there is problem of delay.

6. These systems are sensitive to noise.

7. These devices are not independent [15].

4. Results and discussions

4.1 Generation of keys

The sender decides large sequence of binary bits, which are polarized on a random choice of rectilinear (0, 90 degree) and diagonal basis (45, 135 degree). Binary bits are encoded according to the table shown (**Table 2**).

Bit	**0**	**0**	**1**	**1**
Base	+	X	+	X
Orientation	—	\	|	/

Table 2.
Representation of binary bits.

Encoded keys are transmitted as polarized photons through a quantum channel. Similarly receiver has to measure these polarized photons since the receiver does not have idea about the basis used by sender, receiver randomly chooses between diagonal and rectilinear basis. There are chances of receiver choosing wrong basis which results in misinterpreting the bit received. Once all the bits are received to clarify the bits used sender and receiver communicates over classical channel, and discusses the basis used to polarize each bit. Finally once sender and receiver reveals basis used for polarizing each bit they ignore all the photons for which receiver uses wrong base and consider only those bits that were decrypted using the same base as used by sender. In short, sender and receiver on a common basis generate key of shorter sequence of bits (**Table 3**).

Sender's bit	**0**	**1**	**0**	**1**
Base	+	+	X	X
Orientation	—	|	\	/
Receiver base	+	X	X	X
Received bit	0	0	0	1

Table 3.
Comparison measurements.

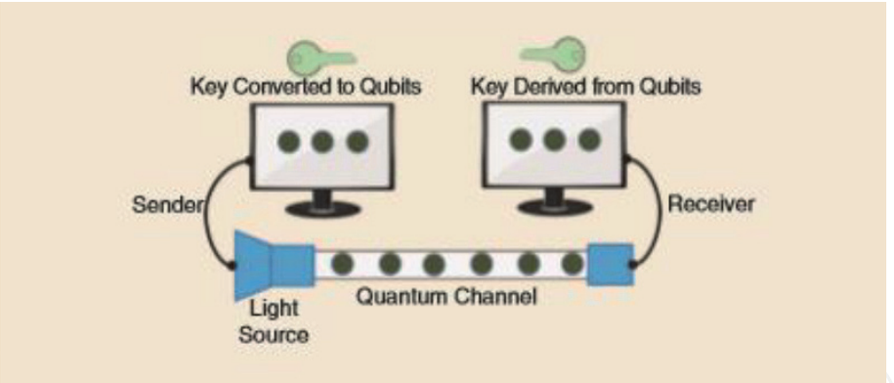

Figure 7.
Illustration of QKD.

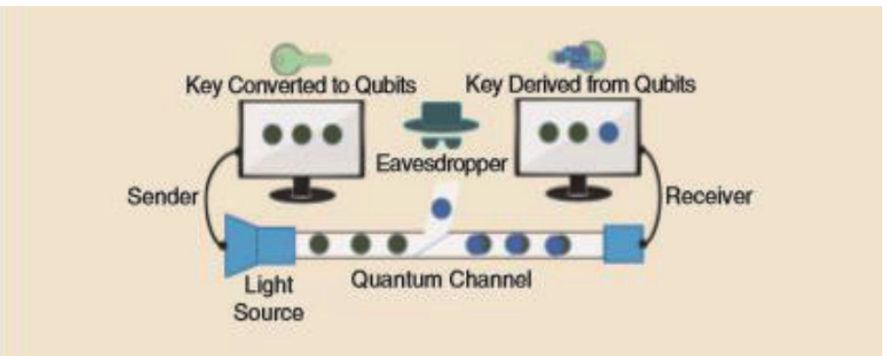

Figure 8.
Impact of eaves dropping on QKD.

The bits for which receiver uses wrong basis are discarded and the remaining bits are considered as key. QBER (Quantum Bit Error Rate) is measured for the chosen key and if its less than threshold value, in that case key is used for message encryption, else key is discarded and is expected for another key transmission (**Figures** 7 and **8**).

Quantum key distribution is not a replacement for the present day cryptography, but a more secured way of transmitting keys which are required for a encoding and decoding of the messages. The maximum speed and the amount of information that can be sent using quantum key distribution is not very large. But it is very secure [16, 17].

Sending:

1. After deciding number of bits to exchange, Alice decides the stream of basis (rectilinear or diagonal) for each pulse of photons she is going to send. A lot of this bits are discarded later due to mismatch of basis, so the Main aim is not to transfer a specific key, but to agree on a common key.

2. Desired polarized Photons are generated using A light-emitting diode (LED) Or from a laser. Each pulse consists of a single Photon. In real-time it has to be a beam of light whose intensity is has to be maintained with care. Because if the intensity is too low, the receiver might not be able to detect the pulse of photon. Also, if the intensity is too high, then the eaves dropper can measure the beam of light with respect to both the basis without letting his presence known to the user as there will be no major change made to the spin. So, there as to be a threshold to be set for beam of light.

Receiving and converting.

3. Bob, who is the exclusive receiver of the information, choses stream of basis (rectilinear or diagonal) to measure the spin of each photon.

4. Number of basis used in receiver end is also predetermined and equal to number of bits that was decided to be exchanged (**Figures 9** and **10**).

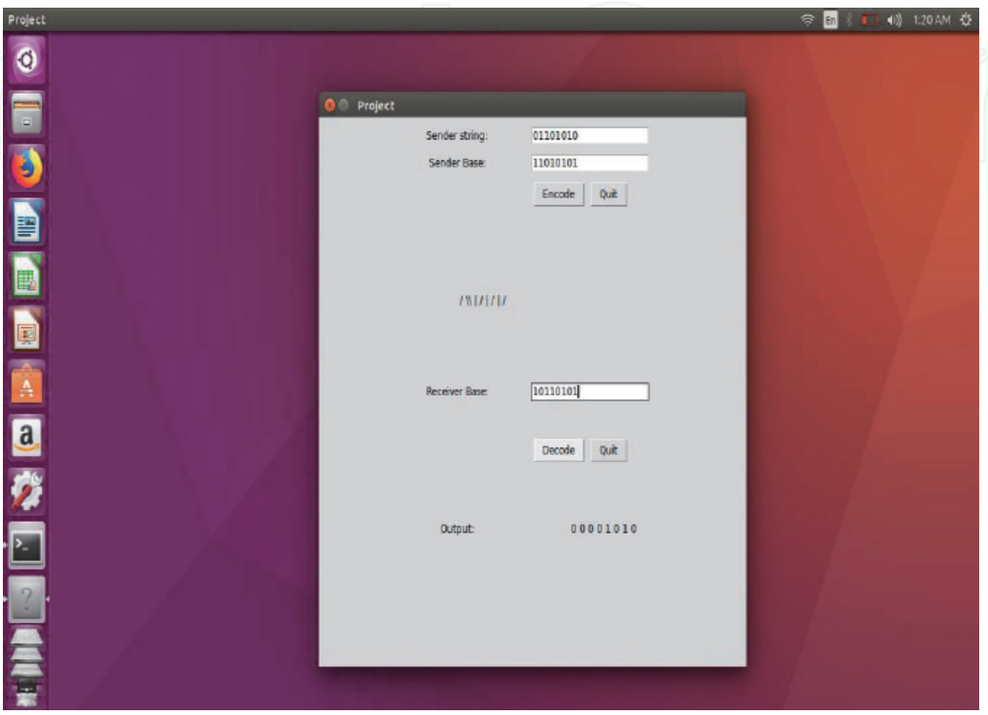

Figure 9.
Receiver entering the basis and decodes key.

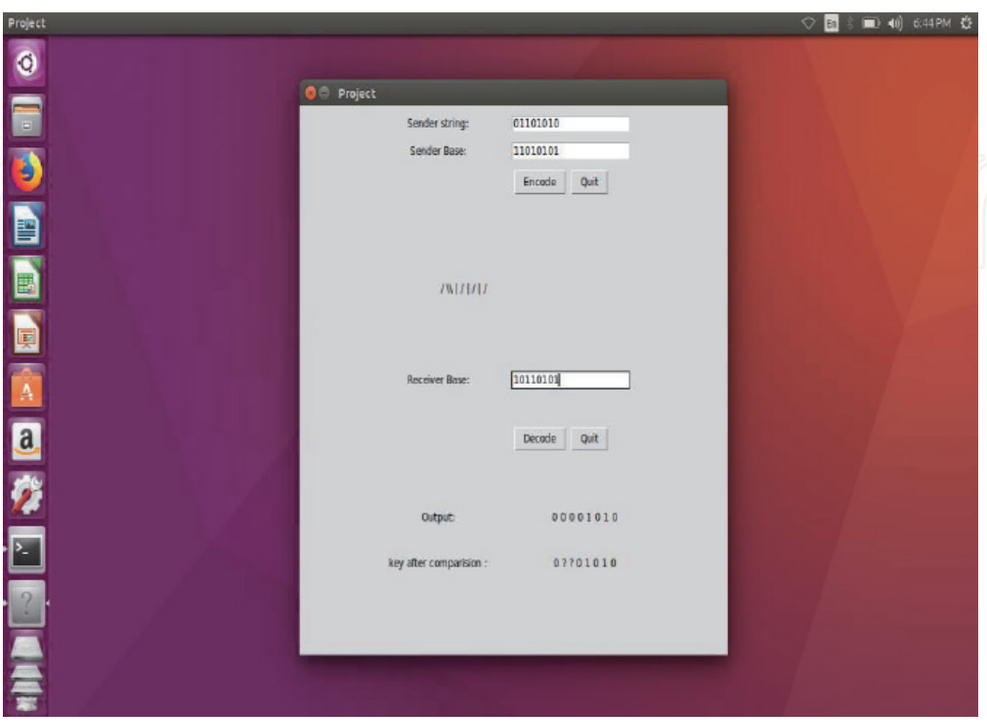

Figure 10.
Results key after discarding mismatched bits.

5. Now, Bob will announce the basis that he used to receive each photon on a public channel without giving much attention if other people are hearing it.

6. Now, Alice publically announces the basis which has matched.

7. All the unnecessary bits whose basis was not matched are discarded.

8. Bits received through the correctly-chosen basis are now converted on to binary code.

9. Using the bits that have matched as keys, the actual plain text is encoded and sent over a public Channel without worrying about eavesdropping.

5. Applications

1. **Ultra-Secure Voting:** To detect and control voter fraudulent during elections, a more secured system is desired. By using Quantum cryptography the voting results are kept secured. Especially the important vulnerable part of the data transaction is uninterruptible. This technology is expected to escalate worldwide, as fraudulent elections may be faced by many countries.

2. **Secure Communications with Space:** Secure space communications with satellites and astronauts is of major concern. NASA is working on a project, with Quintessence Labs to guarantee the security of communication.

3. **Smarter Power Grid:** Normally power grids are at more risk, due to cyber-attacks. Smart grids are required for stabilizing the supply and demand. With adequate precautions, they are more efficient than the traditional grids. With Quantum cryptosystems, it is be possible to preserve the safety of the framework against any attacks.

4. **Quantum Internet:** Internet needs to be relatively fast and secured. By using Quantum cryptosystem, the speed of the internet greatly slows down. If the switching between the q-bits can be done at a significantly faster rate, then the sensitive data over the internet can be more secured and can be retrieved quickly.

6. Conclusion

In this article, the key distribution algorithm using quantum mechanics and concepts of physics is elaborated. Using famous BB84 algorithm and python programming, the system can successfully transfer the secret key from sender to receiver. Along with automatic generation and transmission of Qbits, a GUI can be designed for a user to send bits of their choice. Also the photon orientations/spin can be depicted in the transmission from sender end to receiver end. Quantum Cryptography is mainly designed to be future ready Quantum computer to face threats. It performs exceptionally well without any rigorous and complex mathematical calculations. At the receiver end the photons are received in an expected manner and provide accurate data to the user. The main advantage being 0% exposure of information to intruders and Quantum computers are efficient in transferring keys. The physical implementation which is still a challenge needs lot of

meticulous work to setup the system. Long distance transmission is limited as the photons might lose its energy. As the whole system is performing accurately up to this mark, error bit calculation and notifying the exclusive users about the presence of Eavesdropper is proposed as a future work. Any attempts to attack the communication will be notified to the user through error rate being higher than threshold.

Acknowledgements

We would like to take this opportunity to thank all those who were kind enough to provide assistance when needed, which helped us in completing this article. We are grateful to the management of Dayananda Sagar College of Engineering, for their kind co-operation. We would like to express our heartfelt thanks to our beloved head of the department, Dr. A R Aswatha, for his constant encouragement and timely suggestions during the course of preparation of the article. We are very grateful to Dr. Nagamani A N, post-doctoral from IISc, Bangalore, Karnataka, India for her constant supervision, motivation and support provided during the completion of the article. We would like to thank Almighty, our parents for their support and encouragement throughout the work.

Author details

Bharadwaja V. Srividya and Smitha Sasi*
Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

*Address all correspondence to: smitha.sasi24@gmail.com

IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] William Stallings, "Cryptography and Network Security", Edition 4, Pearson Publishers

[2] Logan O. Mailloux, Charlton D. Lewis II, Casey Riggs, and Michael R. Grimaila, "PostQuantum Cryptography What Advancements in Quantum Computing Mean for IT Professionals", IEEE 2016

[3] Harshad R. Pawar, Dr. Dinesh G. Harkut, "Classical and Quantum Cryptography for Image Encryption & Decryption", IEEE 2018

[4] C. G. Almudever; L. Lao; X. Fu; N. Khammassi; I. Ashraf; D. Iorga; S. Varsa mopoulos; C. Eichler; A. Wallraff; L. Geck "The engineering challenges in quantum computing" , Design, Automa tion & Test in Europe Conference & Exhibition (DATE), 2017

[5] Ashish Nanda, Deepak Puthal, Saraju P. Mohanty, and Uma Choppali, "A Computing Perspective on Quantum Cryptography", IEEE Consumer Electronics Magazine 2018

[6] Xiongfeng Ma, Hongyi Zhou, Kefan Lv, "Security level and information flow in a quantum key distribution network", IEEE 2018

[7] Songsheng Tang, Fuqiang Liu, "A one-time pad encryption algorithm based on one-way hash and conventional block cipher", IEEE 2012

[8] Farzan Jazaeri; Arnout Beckers; Armin Tajalli; Jean-Michel Sallese, "A Review on Quantum Computing: From Qubits to Front-end Electronics and Cryogenic MOSFET Physics", 2019 MIXDES - 26th International Conference "Mixed Design of Integrated Circuits and Systems"

[9] Huber Nieto-Chaupis, "Encrypted Communications through Quantum Key Distribution Algorithms and Bessel Functions", IEEE 2018

[10] P. Siva Lakshmi, G. Murali, "Comparison of Classical and Quantum Cryptography using QKD Simulator", IEEE 2017

[11] Ankur Raina and Shayan Garani Srinivasa, "Eavesdropping on a quantum channel with a unitarily interacting probe", IEEE 2015

[12] D N Kartheek, G Amarnath, P Venkateswarlu Reddy, "Security in Quantum computing using quantum key distribution protocols", IEEE 2013

[13] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Comput*, vol. 26, no. 5, pp. 1484-1509, Oct. 1997, [online] Available: http://dx.doi.org/10.1137/S0097539795293172.

[14] Ali Ibnun Nurhadi, Nana Rachmana Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey", IEEE 2018

[15] Soumy jain" Quantum computer architectures: A survey", IEEE 2nd Inte rnational Conference on Computing for Sustainable Global Development (INDIACom) 2015

[16] Masahide Sasaki, "Quantum Key Distribution and Its Applications", IEEE 2018

[17] J. Aditya, P. Shankar Rao "Quantum Cryptography", https: //cs.stanford.edu/people/adityaj/Quantum Cryptography.pdf